Cybersecurity Benefits of Executive Order 13,694

William Augustine
Department of Informatics
The University at Albany
Albany, New York 12222 USA
Email: WAugustine@albany.edu

Abstract—On April 1, 2015, President Obama issued Executive Order 13,694 entitled “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities” Is America safer because of this? This paper looks at the environment in which this Executive Order is intended to operate (including what may be meant by certain persons and significant malicious activities) and how it may aid the fight against cybercrime and cyberterrorism.

I. INTRODUCTION

Among the duties of the United States President, as the head of the executive branch of the government, is the responsibility to “take Care that the Laws be faithfully executed” [1]. One means of discharging this duty is through the use of Executive Orders. Executive Orders are directives from the President to the agencies which report to the executive branch [2], such as the Department of the Treasury. The issuance of Executive Orders is not intended to create law, but rather to influence an interpretation and enforcement of the nation’s existing laws. They have been issued by every President since George Washington[1]. Some have had more historical significance than others; it was through Executive Order that President Roosevelt ordered the internment of U.S. citizens of primarily Japanese descent [3] and in 1861 it was by Executive Order that President Lincoln suspended the writ of habeas corpus[2].

In a February 2015 press release, the White House said that “[c]yber threats are among the gravest national security dangers to the United States” [4]. Less than two months later, on April 1, 2015, President Barack Obama issued an Executive Order [5] to add an additional means of protecting American interests against “certain persons engaging in significant malicious cyber-enabled activities”. This was done because, as chief executive, he “bears no greater responsibility than ensuring the safety and security of the American people” [6]. To understand what this Executive Order means, we will need to understand what “significant malicious cyber-enabled activities” are and who the “certain persons” might be. An understanding of the threat posed to society and the expectations for improved security will follow.

II. THE INTERNET THREAT ENVIRONMENT

1) Certain Persons: A cyberattack might be launched by an individual or group to further their own ends, or by an agent of a foreign power as an element of international conflict. The distributed and ubiquitous nature of the Internet means that the cyber-enabled activities of either type of actor could be enacted from and targeted to just about anywhere in the world. There are as many as 15 ways to identify the types of individuals or non-state-sponsored groups who commit these cyberattacks. These include organized crime and terrorist groups as well as others which fall under monikers such as hacker, hacktivist, script kiddie and scammer [7]. These acts could be driven by any combination of political interests, financial gain and emotion, among other motives.

State sponsored actors are becoming an integral part of the cyberwarfare and cyberdefense capabilities being built by many nations. The United States Cyber Command reached full operational capability on October 31, 2010 with a directive to “conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries” [8]. The U.S. is not alone in the militarization of cyberspace. “China, India, and Russia alongside the U.S., the U.K. and South Korea are among the first group of countries to establish formal command and control (C2) over military assets in the cyber-domain” [9, p523].

It can be difficult to identify those persons who are engaged in cyberattacks or to determine their motives and affiliations. Appropriate requital requires accurate attribution. Even if the personal identity of a cyberattacker was unequivocally determined, what level of retribution is acceptable? Might it differ depending on the level of damage caused? What if they are located outside of one’s territorial borders? Is it different if they were acting under the orders of a foreign government, and could that even be determined? There is reason to believe that state sponsored cyberattacks have already been launched.

Some accuse national governments (particularly Russia, China, and the tandem of U.S. and Israel) of having already employed cyberattacks against other countries. Former Soviet nations experienced computer disruptions just prior to Russian military operations. “Russia has been implicated in several recent, high-profile cyberattacks, including those against Kyrgyzstan, Lithuania, Chechnya, Estonia, and Georgia. In most cases, no definitive evidence tied the Russian government to these attacks” [10, p18]. Those behind the massive online espionage incidents labeled Titan Rain, in 2003, and GhostNet, in 2009, have been traced back to China. “Although researchers investigating the GhostNet attacks have been unable to tie
them directly to China or any other state, evidence suggests that these attacks were state sponsored at some level” [10, p17]. Reports have accused the U.S. and Israel of working in concert to develop and deploy the Stuxnet worm with the intent of disrupting Iran’s nuclear program [11, p1082]. These are just some of the ways that the internet has enabled cyber activities and exemplifies how difficult it is to appropriately assign blame.

These examples have focused on sources of foreign origin for a reason. For the purposes of Executive Order 13,694, “certain persons” applies to those “located, in whole or in substantial part, outside the United States.”

2) Cyber-Enabled Activities: The Internet has radically changed the way that organizations interact with their clients in both the public and private sectors. It has done so by creating a means of communication that is world-wide and immediate. The resulting flow of information and money (which are not necessarily distinct) no longer knows limitations of national borders and thus falls into no single, well described legal jurisdiction. The interactions within these markets and forums occur in cyberspace. Wherever money and power are parleyed, there will be crime, and cyber-enabled activities will give rise to cybercrime. This “where” does not exist physically and therefore no universal agreement exists regarding how to go about policing such a transnational and ethereal dominion. No nation has the mandate providing legitimate authority.

Making this more difficult still is the fact that even among key stakeholders in Internet security (such as legal experts, academics and cybersecurity practitioners) there does not exist a single accepted definition of what constitutes cybercrime [12]. Whose statutes are in effect: those governing where the perpetrator physically was at the time of the crime, wherever the communication flow passed, or where the victim was? If no one can claim control of the ephemeral realm of cyberspace, should it have its own laws and, if so, who would enforce them?

Similar to the vagaries surrounding cybercrime, there is no definitive meaning for the term cyberterrorism. “[N]o single definition of cyberterrorism is agreed upon by all, in the same way that no single, globally accepted definition of classical political terrorism exists” [13, p3]. One does not need to look at this on a global scale to see the problem. The FBI and the U.S. Department of State have different definitions of terrorism. “Even the U.S. government cannot agree on one single definition” [14, p1]. The difficulties in differentiating criminal activity from those that are terror-related in the physical world mirror the issues defining cybercrime and cyberterrorism.

Whatever the official definition, a 2014 Pew Research study showed that a majority of the experts surveyed believed that in the next decade there will be a major cyberattack resulting in “widespread harm to a nation’s security and capacity to defend itself and its people” [15, p6]. This attitude is also reflected by the law enforcement community. Addressing the Senate Judiciary Committees Subcommittee on Crime and Terrorism, FBI Cyber Division Assistant Director Gordon Snow stated that “[a]s the subcommittee is aware, the number and sophistication of cyber attacks has increased dramatically over the past five years and is expected to continue to grow” [16]. “The Federal Bureau of Investigation (FBI) considers high-tech crimes to be the most significant crimes confronting the United States” [17].

When “certain persons”, regardless of whether they are under the direction of a foreign government, engage in “significant malicious cyber-enabled activities”, those activities can be classified within four types of action: use, misuse, offensive use and cyberterrorism [13, p276]. Each of these differs in the way they are employed and the types of damage that might be dealt to susceptible targets.

3) Susceptible Targets: Computer technology can be used as a communication tool to recruit, train, mobilize and coordinate the activities of the participants of a cyber-enabled activity. This constitutes the first action within the Conway typology—use—and targets people to influence them to become involved in the activity in ways ranging from fundraising through direct action. Terrorist groups, such as Hamas and Hezbollah, use websites, online chat groups and email to radicalize and organize new adherents. They post propaganda to incite violence and provide instructions on how to build bombs and launder money [13, p277].

Misuse and offensive use involve computers attacking computers. These actions are often the result of compromises caused by attack software (a.k.a. malware). Malware comes in many forms (e.g. virus, buffer overflow) and delivery methods (e.g. infected email, vulnerable server software). Sometimes the malware leaves control software on the infected computer so it can later be remotely controlled and joined to a botnet.

Misuse of computers involves the disruption of legitimate cyber-enabled activities. This can be through the defacement of web sites or by using denial of service (DoS) attacks. Inadvertent DoS conditions can be the effect of propagating malware. The Blaster worm may have contributed to the severity of the 2003 Northeast blackout that left over 50 million people in Canada and the U.S. without power [18]

Given how reliant corporations have become on computers (some businesses do not even have a physical presence) attacks against networks could have devastating economic effects; consider the effect of a successful attack on a stock exchange. Offensive use of the Internet includes using technology for theft, such as identity theft, account siphoning, or copyright infringement.

The fourth action in the Conway typology is cyberterrorism, which means using Internet technologies to cause physical harm. This is the rarest form of cyberattack, but the one that could wreak the most havoc. There have only been two confirmed fully-cyber attacks that resulted in physical destruction [19]. The first was the Stuxnet worm that caused damage to centrifuges in the Iranian nuclear facility at Natanz. Only recently, a second event at a German steel plant caused

---

A collection of infected computers (called zombies) that a hacker can remotely take control of to act en masse.
massive damage to a blast furnace. Neither incident resulted in personal injury.

Given how much critical infrastructure is controlled by computer it may only be a matter of time before more of these occur and eventually result in bodily harm or loss of life. SCADA\(^4\) systems manage a wide array of functions such as air traffic control, ground traffic signals, and municipal water processing. If a cyberterrorist group could compromise an active nuclear power facility or weapons control system, a truly terrifying event could result. "The more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructures" [20, p.1].

III. THE STATE OF U.S. CYBER-SECURITY POLICY

So far, the majority of targets of "significant malicious cyber-enabled activities" have been private sector entities and individuals. These are dealt with using the same legal framework as employed in the physical world. "The United States does not have a national strategy exclusively focused on combating cybercrime. Rather, there are other, broader strategies that have cybercrime components" [17, p.16].

Incidents with an international component necessitate federal government involvement. In the case of the 2014 Sony hack (widely considered a reaction to the movie "The Interview") the FBI determined that the attack was state-sponsored. In response, the President issued an Executive Order imposing additional economic sanctions against the North Korean government [21]. This scenario demonstrates again the difficulties inherent in attribution for acts in cyberspace. There are computer security experts who dispute that North Korea was behind the computer compromise and release of the Sony emails and instead believe it may have been perpetrated by disgruntled former employees [22].

In a theater of wartime operations the stakes are far greater than in the movie theater. Insurgent forces in Iraq have been found in possession of video feeds from U.S. military predator drones. They were able to hack into the video surveillance communication streams sent from the drones to their operational base [23]. Virus code has been detected on computers that serve as command and control consoles for military drones [24]. Even after multiple attempts to remove the malware it continued to persist. To this point, Air Force network security specialists have considered it benign, but just consider the scenario where hostile forces were able to take remote control of our drones (as is done with botnets) and turn them against U.S. or allied troops.

IV. WHAT THIS EXECUTIVE ORDER PROVIDES

Executive Order 13,694 does not address securing cyberspace against the most potentially damaging effects resulting from "significant malicious cyber-enabled activities". The lack of focus on prior restraint does not mean that it is without reason. The particulars of this Executive Order are consistent with the way in which cyber-enabled activities have been dealt. "[M]any of these so-called cybercrimes can be easily likened to traditional crimes...criminals are often prosecuted using laws intended to combat crimes in the real world" [17, p.4]. Asset forfeiture is one such tactic that is employed to combat crimes in the real world. There are strong similarities in the structure of organized crime syndicates and terrorist groups. Federal forfeiture statutes exist in order to suppress the ability of criminal organizations from using their ill-gotten gains to improve their defense against prosecution (both criminally and civilly) and provide recompense to injured parties. These are Racketeer Influenced and Corrupt Organizations statutes, a.k.a. RICO [25]. This provides for the ability of the government to seize any assets that are involved, in part or in whole, in the commission of criminal activity. In 2013, RICO was first used in the fight against online crime [26].

Forfeiture statutes when applied against terror organizations were strengthened by the Patriot Act [27]. All assets belonging to someone involved in terrorism (either domestically or internationally) are acceptable targets for seizure and forfeiture regardless of whether those assets were involved in the planning or commission of an act of terror. The Patriot Act also provides an impediment to terror funding by applying RICO provisions to those involved in reverse money laundering\(^5\).

If Patriot Act strengthened RICO statutes already allowed for "blocking the property of certain persons engaging in significant malicious cyber-enabled activities" what was gained in Executive Order 13,694? Under previous interpretation of these laws judicial action was required before a law enforcement agency would be allowed to seize assets. Now, assets can be seized from these "certain persons" as determined "by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State". This shows that, according to the President, searches and seizures when in suppression of terrorist activity are not considered unreasonable in terms of the Fourth Amendment to the Constitution [28].

V. CYBER POLICIES BEYOND THE U.S.

Although the U.S. created the Internet, Americans are not alone in cyberspace and the difficulty in securing one's interests is shared by all nations. Each nation will have its own laws influencing the interpretation of cybercrime and cyberterror, as will multi-national bodies. Cybersecurity will need to be an international effort because of the ubiquitous nature of the Internet.

In 1999, the United Nations issued its Manual on the Prevention and Control of Computer Related Crime [29]. An attempt to define cybercrime was included and it called for further cooperation among nations, including a harmonization of laws and the creation of a jurisdictional entity for cyberspace. There was never a binding agreement reached as a result of these efforts.

\(^4\)Supervisory Control And Data Acquisition: systems that monitor and control hardware such as those in a manufacturing plant or telecommunications facility.

\(^5\)Money laundering is the process of disguising the true source of proceeds gained from illegal activities. Reverse money laundering is disguising the source of legitimate money intended to fund illegitimate (e.g. terror-related) activities.
The oldest multinational agreement addressing this topic is the Council of Europe’s Convention on Cybercrime, a.ka. the Budapest Convention. Participation in this effort was extended to nations beyond the 45 members of the Council of Europe. This agreement was meant to create an accepted definition of cybercrime and provide for greater cooperation in the investigation and prosecution of cybercrimes involving multiple nations [30]. Each of the signatories is expected to draft into their own laws a standard legal framework criminalizing activities such as child pornography, hacking, and violations of intellectual property rights. It went into force on July 1, 2004 and has been signed by 44 nations including the United States, which ratified it in 2006. Russia and China are conspicuously absent from the list of ratifying nations.

Just as there exist unions of nations for economic purposes (such as NAFTA) and for physical security and mutual defense (such as NATO), cooperative “cyber-blocs” of nations sharing a common agenda and cybersecurity strategy have formed. Five in particular are:

- The Anglosphere, led by the US and the UK, emphasizes a leading private sector role, an educated workforce, and outreach and diplomacy.
- The EU, led by Germany, focuses on a robust legal and regulatory framework, and on the promotion of the Council of Europe (Budapest) Convention of Cybercrime as a blueprint for international cooperation and enforcement.
- The Baltic States are in tight cooperation with NATO in the development of their national cybersecurity strategies.
- The post-Soviet CIS bloc, led by Russia with some degree of Chinese cooperation, focuses on internal threats, abhors extra-territorial judicial action, and promotes a corresponding international framework under the auspices of the UN.”

And we can possibly add in another bloc:

- The Nordic States, led by Finland, aiming for practical cooperation in building a common cyber security strategy (with common laws) and supporting each other to develop the necessary capacity to build a defensive coalition.” [31, p147-148].

Global Jus in Bello agreements exist defining the acceptable use of force and limitations on types of weapons allowed in the physical world. “The dangers are so great that cyber arms qualify as weapons of mass destruction” [32, p283]. What are needed are similar international agreements on what are and what are not acceptable cyber-enabled activities and under what conditions their uses are approved. “Without a global cyber-warfare non-aggression pact, it will be impossible to distinguish whether a cyberattack is state sponsored or independent terrorism” [15, p31].

VI. EXPECTED EFFECTIVENESS

In November 2014, months before the passage of Executive Order 13,694, the U.S. employed forfeiture statutes in the fight against online cybercrime. This was prosecuted by the U.S. Department of Justice in concert with 16 international entities toward the closure of Silk Road 2.0 and other dark web market sites [33]. Without using Executive Order 13,694 and even without international cooperation, foreign companies that do business in the United States can be susceptible to forfeiture through legal rather than diplomatic channels. The French bank, BNP Paribas S.A., was “ordered to forfeit $8,833,600,000 to the United States and to pay a $140,000,000 fine” for deliberately evading U.S. sanctions against Sudan, Iran and Cuba[34].

A potential way to evaluate the efficacy of a deterrence effect of this Executive Order is to perform a hypothesis test using attack statistics. We will assume that there is no difference in the number of attacks before the order and after.

**Hypothesis 1** There is a difference in the number of attacks before and after the Executive Order.

Using cyber attack statistics for January 2014 through March 2016, inclusive, as reported by Hackmageddon.com⁶, results (shown in Table 1) from a paired two-tailed t-test fail to reject H₀. A Kolmogorov-Smirnov comparison found the two samples were both normally distributed. Additionally, calculating for PreEO<PostEO reveals a *p*-value = 0.9915 meaning that it is statistically significant that there were typically fewer attacks in the months prior the Executive Order than those following to it. Further investigation reveals that the percentage related to cybercrime was also higher (with fewer attributed to hacktivism). This is highly circumstantial and should not be interpreted as implying causation; there is no saying that without Executive Order 13,694 the numbers would have been even higher and due to the time periods used an autocorrelation effect could be present.

**TABLE 1**

| Attack Deterrence Statistics Pre-Executive Order vs. Post-Executive Order. |
|---|---|---|---|---|
| Period | N | Mean | StDev | St Mean |
| PreEO | 15 | 76.067 | 9.7469 | 2.521 |
| PostEO | 13 | 84.538 | 7.4458 | 2.065 |

Laws exist for preventive, curative and facilitative functions in order to dissuade behaviors, to punish those that decide to transgress the law, and to support social institutions, respectively[35, p234]. The previous paragraph addressed the case of prevention. In regard to the second, ex post facto form, as of the writing of this paper, Executive Order 13,694 has not been cited in any court cases. In this analysis, there is no reason for consideration of the facilitative form.

If one is inclined to believe in the power of economic sanctions then the provisions of this Executive Order should be expected to assist in effectively suppressing “malicious cyber-enabled activities”, although from the cases against Silk Road 2.0 and BNP Paribas S.A. they are not necessary for it. In fact, according to the World Trade Organization (WTO) this order

is unnecessary if the President decides to assess sanctions in the event of “significant malicious cyber-enabled activities”. “WTO members have successfully argued that the WTO Dispute Settlement Body (DSB) has no authority when sanctions are imposed for national security reasons”[36, p1485]. “It is agreed, however, that online activities substantially improve the ability of such terrorist groups to raise funds, lure new faithful, and reach a mass audience” [13, p277]. It might be expected that asset seizure will help materially reduce the ability of "certain persons" to function in these ways. An investigation by the GAO into the effectiveness of the first decade of RICO forfeiture in the war on drugs found that "neither the dollar value nor the type of assets forfeited to the Government by criminal organizations has been impressive compared to the billions generated annually through drug trafficking."[37, pi-ii].

More questions than answers have been presented here, but one more question in particular needs to be posed: in the past year, has Executive Order 13,694 made the U.S. safer? There appears to be reason to believe that there are no cyber-security benefits to Executive Order 13,694 although the President of the United States declared a state of emergency to enact it.

ACKNOWLEDGMENT
Gratitude is due to Dr. Deborah Andersen of the University at Albany for guidance, instruction and editorial prowess. All writing errors in this version are attributable to the author alone. John Moore, Esq. provided expert legal guidance and any misinterpretations are (again) solely the fault of the author.

REFERENCES